



PATENT ABSTRACTS OF JAPAN

(11) Publication number: **2002032340 A**(43) Date of publication of application: **31.01.02**

(51) Int. Cl.

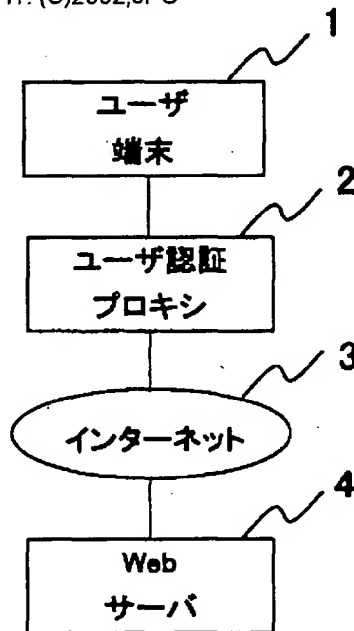
G06F 15/00**G06F 12/14****H04L 9/32**(21) Application number: **2000214625**(71) Applicant: **NEC CORP**(22) Date of filing: **14.07.00**(72) Inventor: **AZUMA TOMIHIKO**(54) **SYSTEM AND METHOD FOR SINGLE SIGN-ON
WEB SITE AND RECORDING MEDIUM**terminal, when the received data coincide with the
stored data.

(57) Abstract:

COPYRIGHT: (C)2002,JPO

PROBLEM TO BE SOLVED: To provide a system and a method for reducing the load of a user by representively performing user authentication to an optional Web site requiring user authentication.

SOLUTION: A user authentication proxy 2 provided between a user terminal 1 and a Web server 4 stores the URL of a Web site as information related to a series of user authentication processes performed by the user with the Web server by utilizing the user terminal, data which the user terminal receives from the Web server for the user authentication, and data for user authentication which the user terminal transmits to the Web server for user authentication. When receiving data for a URL from a Web server indicated by the URL, when the user designates the URL of the Web site by using an optional user terminal, the proxy 2 compares the received data with the received data that are stored, does not transfer the received data from the Web server and but transmits stored transmission data for user authentication to the Web server in place of the user



(19)日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11)特許出願公開番号

特開2002-32340

(P2002-32340A)

(43)公開日 平成14年1月31日(2002.1.31)

(51)Int.Cl. ⁷	識別記号	F I	テマコード(参考)
G 0 6 F 15/00	3 3 0	G 0 6 F 15/00	3 3 0 B 5 B 0 1 7
12/14	3 2 0	12/14	3 2 0 A 5 B 0 8 5
H 0 4 L 9/32		H 0 4 L 9/00	6 7 3 A 5 J 1 0 4

審査請求 有 請求項の数10 O L (全 12 頁)

(21)出願番号 特願2000-214625(P2000-214625)

(22)出願日 平成12年7月14日(2000.7.14)

(71)出願人 000004237

日本電気株式会社

東京都港区芝五丁目7番1号

(72)発明者 東 富彦

東京都港区芝五丁目7番1号 日本電気株式会社内

(74)代理人 100080816

弁理士 加藤 朝道

Fターム(参考) 5B017 AA03 BA09 BB09 CA15 CA16

5B085 AE02 AE23

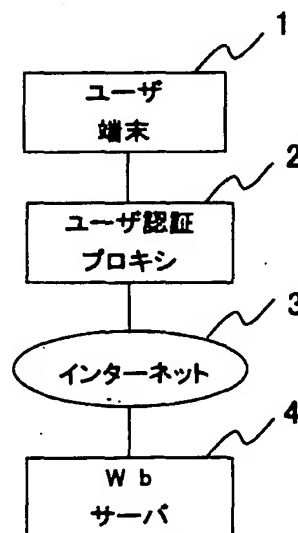
5J104 AA07 KA01 NA05 PA07

(54)【発明の名称】 Webサイトに対するシングルサインオンシステム及び方法並びに記録媒体

(57)【要約】

【課題】ユーザ認証を必要とする任意のWebサイトに対して、ユーザ認証を代行することで、ユーザの負担を軽減するシステム及び方法の提供。

【解決手段】ユーザ端末1とWebサーバ4との間に設けられたユーザ認証プロキシ2が、ユーザがユーザ端末を利用してWebサーバとの間で行った一連のユーザ認証プロセスに係わる情報としてWebサイトのURL、ユーザ認証用にユーザ端末が前記Webサーバから受信したデータ、ユーザ認証用にユーザ端末がWebサーバへ送信したユーザ認証用データを保存し、ユーザが任意のユーザ端末を利用してWebサイトのURLを指定した場合、該URLで指示されるWebサーバから該URLに対するデータを受信した際に受信データと保存されている受信データを比較し、等しい場合にWebサーバからの受信データをユーザ端末に転送せず、保存されているユーザ認証用の送信データをユーザ端末に代わってWebサーバに送信する。



【特許請求の範囲】

【請求項1】 インターネットを介してWebサーバにアクセスするユーザ端末と、前記Webサーバとの間に、Webサイトにおけるユーザ認証を代行するユーザ認証プロキシ装置を備え、

前記ユーザ認証プロキシ装置は、ユーザ認証を代行するために必要なデータを記録する手段を備え、

ユーザ端末で指定したWebサイトに対するユーザ認証を前記ユーザ認証プロキシ装置に代行させ、前記ユーザ端末におけるユーザ認証のための操作を削減する、ことを特徴とする、Webサイトに対するシングルサインオンシステム。

【請求項2】 前記ユーザ認証プロキシ装置は、ユーザ認証時に前記ユーザ端末と前記Webサーバとの間で送受信されるデータを記憶手段に保存し、ユーザ認証の代行時、前記記憶手段に記憶されているデータを再利用する、ことを特徴とする、請求項1記載のWebサイトに対するシングルサインオンシステム。

【請求項3】 インターネットを介してWebサーバにアクセスするユーザ端末と、前記Webサーバとの間にユーザ認証プロキシ装置を備え、

前記ユーザ認証プロキシ装置は、ユーザがユーザ端末を利用してインターネットを介して前記Webサーバとの間で行った一連のユーザ認証プロセスに係わる情報として、WebサイトのURL (Uniform Resource Locator)、ユーザ認証用に前記ユーザ端末が前記Webサーバから受信したデータ、ユーザ認証用に前記ユーザ端末がWebサーバへ送信したユーザ認証用データの3つのデータを組として記憶手段に保存する手段と、

前記ユーザが任意のユーザ端末を利用して前記WebサイトのURLを指定した場合、前記URLで指示されているWebサーバに接続要求を送信し、前記Webサーバから該URLに対するデータを受信した際に、前記受信データと、前記記憶手段にあらかじめ保存されている受信データとを比較し、両者が等しい場合には、前記Webサーバからの受信データを前記ユーザ端末に転送せず、前記記憶手段にあらかじめ保存されているユーザ認証用の送信データを、前記ユーザ端末に代わって、前記Webサーバに送信する手段と、を備えた、ことを特徴とするWebサイトに対するシングルサインオンシステム。

【請求項4】 インターネットを介してWebサーバにアクセスするユーザ端末と、前記Webサーバとの間に配設されるユーザ認証プロキシ装置が、

ユーザがユーザ端末を利用してインターネットを介して前記Webサーバとの間で行った一連のユーザ認証プロセスに係わる情報として、WebサイトのURL (Uniform Resource Locator)、ユーザ認証用に前記ユーザ端末が前記Webサーバから受信

したデータ、ユーザ認証用に前記ユーザ端末がWebサーバへ送信したユーザ認証用データの3つのデータを組として記憶手段に保存する手段と、

前記ユーザが任意のユーザ端末を利用して前記WebサイトのURLを指定した場合、前記URLで指示されているWebサーバに接続要求を送信し、前記Webサーバから該URLに対するデータを受信した際に、前記受信データと、前記記憶手段にあらかじめ保存されている受信データとを比較し、両者が等しい場合には、前記Webサーバからの受信データを前記ユーザ端末に転送せず、前記記憶手段にあらかじめ保存されているユーザ認証用の送信データを、前記ユーザ端末に代わって、前記Webサーバに送信する手段と、

を備えた、ことを特徴とするユーザ認証プロキシ装置。

【請求項5】 インターネットを介してWebサーバにアクセスするユーザ端末と、前記Webサーバとの間に配設されるユーザ認証プロキシ装置が、

前記ユーザ認証プロキシ装置を利用するユーザが正当な利用者であることを確認するために必要な情報として、

利用者を一意に識別するユーザ識別子とパスワードを記憶するプロキシ利用者認証用データ記憶部と、

利用者を一意に識別するユーザ識別子と、WebサイトのURLと、ユーザ認証用にユーザ端末がWebサーバから受信した受信データと、ユーザ認証用に前記ユーザ端末が前記Webサーバに送信した送信データとの組を記憶するWebサイト利用者認証用データ記憶部と、を備えた記憶装置と、

前記プロキシ利用者認証用データ記憶部に保存されているデータを利用して、ユーザがユーザ認証プロキシ装置の正当な利用者であるかどうかの認証を行うプロキシ利用者認証手段と、

ユーザが前記ユーザ認証プロキシ装置にユーザ認証を代行させるように指示したWebサイトのURLを、ユーザを一意に識別するためのユーザ識別子と組にして前記Webサイト利用者認証用データ記憶部に保存するURL保存手段と、

ユーザ認証を行うために前記ユーザ端末が前記Webサーバから受信したデータを、前記Webサイト利用者認証用データ記憶部に保存する受信データ保存手段と、

ユーザ認証を行うために前記ユーザ端末が前記Webサーバへ送信したデータを、前記Webサイト利用者認証用データ記憶部に保存する送信データ保存手段と、

前記ユーザがユーザ端末で指定したURLと、前記Webサイト利用者認証用データ記憶部に保存されているURLとを比較し、前記ユーザ認証プロキシ装置がユーザ認証を代行するURLであるか否かを判断するURL比較手段と、

前記ユーザが指定したURLを使用して前記Webサーバに接続し、前記Webサーバから受信したデータと、前記Webサイト利用者認証用データ記憶部に保存され

ている受信データとを比較する受信データ比較手段と、前記ユーザ識別子、URL、および前記Webサーバから受信した受信データの組が、前記Webサイト利用者認証用データ記憶部に存在する場合には、ユーザ認証の代行が可能であるものと判定し、ユーザ認証を代行するために、前記Webサイト利用者認証用データ記憶部から対応する送信データを取得して前記Webサーバへ送信する代行認証用データ送信手段と、

を備えたことを特徴とするユーザ認証プロキシ装置。

【請求項6】インターネットを介してWebサーバにアクセスするユーザ端末と、前記Webサーバとの間に、Webサイトにおけるユーザ認証を代行するユーザ認証プロキシ装置を配置し、

前記ユーザ認証プロキシ装置は、ユーザ認証を代行するために必要なデータを記録し、

ユーザ端末の種類を問わず、ユーザがURLで指定したWebサイトに対するユーザ認証を、前記ユーザ認証プロキシ装置に代行させるようにしたことを特徴とするWebサイトに対するユーザ認証代行方法。

【請求項7】前記ユーザ認証プロキシ装置は、ユーザ認証時に前記ユーザ端末と前記Webサーバとの間で送受信されるデータを保存し、ユーザ認証の代行時、前記保存されているデータを再利用する、ことを特徴とする、請求項6記載のWebサイトに対するユーザ認証代行方法。

【請求項8】インターネットを介してWebサーバにアクセスするユーザ端末とWebサーバとの間にユーザ認証プロキシを設け、

ユーザがユーザ端末を利用してインターネットを介して前記Webサーバとの間で行った一連のユーザ認証プロセスに係わる情報として、WebサイトのURL (Uniform Resource Locator)、ユーザ認証用に前記ユーザ端末が前記Webサーバから受信したデータ、ユーザ認証用に前記ユーザ端末がWebサーバへ送信したユーザ認証用データの3つのデータを組として記憶手段に保存するステップと、

前記ユーザが任意のユーザ端末を利用して前記WebサイトのURLを指定した場合、前記URLで指示されているWebサーバに接続要求を送信するステップと、

前記Webサーバから該URLに対するデータを受信した際に、前記受信データと、前記記憶手段にあらかじめ保存されている受信データとを比較し、両者が等しい場合には、前記Webサーバからの受信データを前記ユーザ端末に転送せず、前記記憶手段にあらかじめ保存されているユーザ認証用の送信データを、前記ユーザ端末に代わって、前記Webサーバに送信するステップと、を含む、ことを特徴とするWebサイトに対するユーザ認証代行方法。

【請求項9】インターネットを介してWebサーバにアクセスするユーザ端末と、前記Webサーバとの間に配

設されるユーザ認証プロキシ装置が、

(a) ユーザがユーザ端末を利用してインターネットを介して前記Webサーバとの間で行った一連のユーザ認証プロセスに係わる情報として、WebサイトのURL (Uniform Resource Locator)、ユーザ認証用に前記ユーザ端末が前記Webサーバから受信したデータ、ユーザ認証用に前記ユーザ端末がWebサーバへ送信したユーザ認証用データの3つのデータを組として記憶手段に保存する処理と、

10 (b) 前記ユーザが任意のユーザ端末を利用して前記WebサイトのURLを指定した場合、前記URLで指示されているWebサーバに接続要求を送信し、前記Webサーバから該URLに対するデータを受信した際に、前記受信データと、前記記憶手段にあらかじめ保存されている受信データとを比較し、両者が等しい場合には、前記Webサーバからの受信データを前記ユーザ端末に転送せず、前記記憶手段にあらかじめ保存されているユーザ認証用の送信データを、前記ユーザ端末に代わって、前記Webサーバに送信する処理と、

20 の前記(a)及び(b)の処理を、前記ユーザ認証プロキシ装置を構成するコンピュータに実行させるためのプログラムを記録した記録媒体。

【請求項10】インターネットを介してWebサーバにアクセスするユーザ端末とWebサーバとの間に配設されるユーザ認証プロキシ装置が、

前記ユーザ認証プロキシ装置を利用するユーザが正当な利用者であることを確認するために必要な情報として、利用者を一意に識別するユーザ識別子とパスワードを記憶するプロキシ利用者認証用データ記憶部と、

30 利用者を一意に識別するユーザ識別子と、WebサイトのURLと、ユーザ認証用にユーザ端末がWebサーバから受信した受信データと、ユーザ認証用に前記ユーザ端末が前記Webサーバに送信した送信データとの組を記憶するWebサイト利用者認証用データ記憶部と、を備え、

(a) 前記プロキシ利用者認証用データ記憶部に保存されているデータを利用して、ユーザがユーザ認証プロキシ装置の正当な利用者であるかどうかの認証を行うプロキシ利用者認証処理と、

40 (b) ユーザが前記ユーザ認証プロキシ装置にユーザ認証を代行させるように指示したWebサイトのURLを、ユーザを一意に識別するための識別子と組にして前記Webサイト利用者認証用データ記憶部に保存するURL保存処理と、

(c) ユーザ認証を行うために前記ユーザ端末が前記Webサーバから受信したデータを、前記Webサイト利用者認証用データ記憶部に保存する受信データ保存処理と、

50 (d) ユーザ認証を行うために前記ユーザ端末が前記Webサーバへ送信したデータを、前記Webサイト利用

者認証用データ記憶部に保存する送信データ保存処理と、

(e) 前記ユーザがユーザ端末で指定したURLと、前記Webサイト利用者認証用データ記憶部に保存されているURLとを比較し、前記ユーザ認証プロキシ装置がユーザ認証を代行するURLであるかどうかを判断するURL比較処理と、

(f) 前記ユーザが指定したURLを使用して前記Webサーバに接続し前記Webサーバから受信したデータと、前記Webサイト利用者認証用データ記憶部22に保存されている受信データとを比較する受信データ比較処理と、

(g) 前記ユーザ識別子、URL、および前記Webサーバから受信した受信データの組が、Webサイト利用者認証用データ記憶部に存在する場合には、代行認証が可能と判定し、ユーザ認証を代行するための送信データを前記Webサイト利用者認証用データ記憶部から取得し、前記Webサーバへ送信する代行認証用データ送信処理と、

の前記(a)乃至(g)の処理を、前記ユーザ認証プロキシ装置を構成するコンピュータに実行させるためのプログラムを記録した記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、WWW (World Wide Web) サーバの認証の代行システムに関し、特に、任意のWebサイトに対するシングルサインオンシステムに関する。

【0002】

【従来の技術】ユーザ認証を必要とするWebサイトが増加するに従って、ユーザ認証を行うために必要な操作が増加し、ユーザに負担がかかるようになってきた。

【0003】さらに、ユーザは、複数のユーザIDやパスワードを覚えることは、負担となり、また、困難であることから、シングルサインオンシステムが求められている。

【0004】これに対して、特定のWebサイトだけを対象とする形でのシングルサインオンシステムや、PKI (Public Key Infrastructure; 公開鍵インフラストラクチャ) を利用した標準的な方法が利用され始めている。

【0005】なお、例えば特開2000-3334号公報には、ユーザからの要求をゲートウェイで受信して該当する他の情報提供サーバあるいは他のゲートウェイにユーザID/パスワードを変換して送信し、その応答を受信したとき逆変換して要求元に送信し、ユーザからみて1つのユーザIDとパスワードで所望の情報サービスを提供するゲートウェイシステムが提案されている。

【0006】

【発明が解決しようとする課題】しかしながら、この従

来のシステムには、次のような問題点がある。

【0007】特定のWebサイトだけを対象とするシステムでは、任意のWebサイトをそのままの形で、シングルサインオンシステムに加えることはできない。

【0008】そして、Webサイトのユーザ認証方法を変更するか、特定の場所にWebサイトを配置するなど対処が必要となる場合が多い。

【0009】一方、PKIをベースにしたユーザ認証方法を利用するためには、ユーザ端末側に、セキュリティ機能を具備することが必要とされる。

【0010】近時、Webサイトを利用するユーザ端末が、従来のPC (パーソナルコンピュータ) から、携帯電話や携帯情報端末、FAX (ファクシミリ装置) などの端末へ広がるとともに、セキュリティ機能を持たない端末が増加し、すべての端末がPKIに対応することは、事実上、不可能になっている。

【0011】したがって、本発明は、上記問題点に鑑みてなされたものであって、その目的は、ユーザ認証を必要とする任意のWebサイトに対して、ユーザ認証を代行することで、ユーザの負担を軽減するシステム及び方法並びに記録媒体を提供することにある。

【0012】

【課題を解決するための手段】前記目的を達成する本発明は、インターネットを介してWebサーバにアクセスするユーザ端末と、前記Webサーバとの間に、Webサイトにおけるユーザ認証を代行するユーザ認証プロキシを配置し、ユーザ端末の種類を問わず、ユーザがURLで指定したWebサイトに対するユーザ認証を、前記ユーザ認証プロキシに代行させるようにしたものである。

【0013】本発明は、インターネットを介してWebサーバにアクセスするユーザ端末とWebサーバとの間にユーザ認証プロキシ装置を備え、前記ユーザ認証プロキシ装置は、ユーザがユーザ端末を利用してインターネットを介して前記Webサーバとの間で行った一連のユーザ認証プロセスに係わる情報として、WebサイトのURL (Uniform Resource Locator)、ユーザ認証用に前記ユーザ端末が前記Webサーバから受信したデータ、ユーザ認証用に前記ユーザ端末がWebサーバへ送信したユーザ認証用データの3つのデータを組として記憶手段に保存する手段と、前記ユーザが任意のユーザ端末を利用して前記WebサイトのURLを指定した場合、前記URLで指示されているWebサーバに接続要求を送信し、前記Webサーバから該URLに対するデータを受信した際に、前記受信データと、前記記憶手段にあらかじめ保存されている受信データとを比較し、両者が等しい場合には、前記Webサーバからの受信データを前記ユーザ端末に転送せず、前記記憶手段にあらかじめ保存されているユーザ認証用の送信データを、前記ユーザ端末に代わって、前記Web

サーバに送信する手段とを備えている。

【0014】

【発明の実施の形態】本発明は、ユーザ認証が必要な複数のWebサイトを、ユーザ端末から利用するシステムにおいて、Webサーバと、ユーザ端末との間にWebサイトにおけるユーザ認証を代行するプロキシを置き、このプロキシに、Webサイトにおけるユーザ認証を代行させることにより、Webサイトを利用する際に、ユーザがユーザ端末で実行しなければならないユーザ認証作業の操作回数を、大幅に削減するものである。

【0015】本発明は、その好ましい一実施の形態において、図1を参照すると、ユーザ認証プロキシ(2)は、ユーザ認証を代行するために必要なデータを記録する。

【0016】ユーザ認証プロキシ(2)は、ユーザがユーザ端末(1)を利用してインターネット(3)を介してWebサーバ(4)との間で行った一連のユーザ認証プロセスに係わる情報を保存する。

【0017】保存するデータとしては、好ましくは、
・WebサイトのURL(Uniform Resource Locator)、
・ユーザ認証用にユーザ端末(1)がWebサーバ(4)から受信したデータ、
・ユーザ認証用にユーザ端末(1)がWebサーバ(4)へ送信したデータよりなる。

【0018】これら3つのデータの組を保存することにより、ユーザ端末(1)の種類を問わず、ユーザがURLで指定したWebサイトに対するユーザ認証を、ユーザ認証プロキシ(2)に代行させることができる。

【0019】ユーザが任意のユーザ端末(1)を利用してWebサイトのURLを指定した場合、ユーザ認証プロキシ(2)は、URLで指示されているWebサーバ(4)に接続要求を送信し、Webサーバ(4)から該URLに対するデータを受信する。

【0020】ユーザ認証プロキシ(2)は、この受信データと、あらかじめ保存してある受信データとを比較し、両者が等しい場合には、Webサーバ(4)からの受信データをユーザ端末(1)に転送せず、あらかじめ保存されているユーザ認証用の送信データを、ユーザに代わってWebサーバ(4)に返却する。

【0021】本発明は、その好ましい一実施の形態において、インターネットを介してWebサーバにアクセスするユーザ端末とWebサーバとの間に設けられたユーザ認証プロキシにおいて、(a)ユーザがユーザ端末を利用してインターネットを介して前記Webサーバとの間で行った一連のユーザ認証プロセスに係わる情報として、WebサイトのURL(Uniform Resource Locator)、ユーザ認証用に前記ユーザ端末が前記Webサーバから受信したデータ、ユーザ認証用に前記ユーザ端末がWebサーバへ送信したユーザ

認証用データの3つのデータを組として記憶手段に保存する処理と、(b)前記ユーザが任意のユーザ端末を利用して前記WebサイトのURLを指定した場合、前記URLで指示されているWebサーバに接続要求を送信し、前記Webサーバから該URLに対するデータを受信した際に、前記受信データと、前記記憶手段にあらかじめ保存されている受信データとを比較し、両者が等しい場合には、前記Webサーバからの受信データを前記ユーザ端末に転送せず、前記記憶手段にあらかじめ保存されているユーザ認証用の送信データを、前記ユーザ端末に代わって、前記Webサーバに送信する処理と、の前記(a)、(b)の処理は、ユーザ認証プロキシのデータ処理装置(コンピュータ)で実行されるプログラムにより実現され、該プログラムを記録した記録媒体(磁気ディスク、磁気テープ、光ディスク、もしくは半導体メモリ等)から該プログラムをデータ処理装置に読み出して実行することで、ユーザ認証プロキシを実施することができる。

【0022】より詳細には、本発明は、その好ましい一実施の形態において、インターネットを介してWebサーバにアクセスするユーザ端末とWebサーバとの間に設けられたユーザ認証プロキシ装置において、前記ユーザ認証プロキシ装置を利用するユーザが正当な利用者であることを確認するために必要な情報として、利用者を一意に識別するユーザ識別子とパスワードを記憶するプロキシ利用者認証用データ記憶部(221)と、利用者を一意に識別するユーザ識別子と、WebサイトのURLと、ユーザ認証用にユーザ端末がWebサーバから受信した受信データと、ユーザ認証用に前記ユーザ端末が前記Webサーバに送信した送信データとの組を記憶するWebサイト利用者認証用データ記憶部(222)と、を備えた記憶装置(22)と、前記プロキシ利用者認証用データ記憶部(221)に保存されているデータを利用して、ユーザが当該ユーザ認証プロキシ装置の正当な利用者であるかどうかの認証を行うプロキシ利用者認証手段(211)と、ユーザが前記ユーザ認証プロキシ装置にユーザ認証を代行させるように指示したWebサイトのURLを、ユーザを一意に識別するためのユーザ識別子と組にして前記Webサイト利用者認証用データ記憶部に保存するURL保存手段(212)と、ユーザ認証を行うために前記ユーザ端末が前記Webサーバから受信したデータを、前記Webサイト利用者認証用データ記憶部に保存する受信データ保存手段(213)と、ユーザ認証を行うために前記ユーザ端末が前記Webサーバへ送信したデータを、前記Webサイト利用者認証用データ記憶部(222)に保存する送信データ保存手段(214)と、前記ユーザがユーザ端末で指定したURLと、前記Webサイト利用者認証用データ記憶部(222)に保存されているURLとを比較し、前記ユーザ認証プロキシ装置がユーザ認証を代行するURL

であるかどうかを判断するURL比較手段(215)と、前記ユーザが指定したURLを使用して前記Webサーバに接続し、前記Webサーバから受信したデータと、前記Webサイト利用者認証用データ記憶部に保存されている受信データとを比較する受信データ比較手段(216)と、前記ユーザ識別子、URL、および前記Webサーバから受信した受信データの組が、前記Webサイト利用者認証用データ記憶部に存在する場合には、代行認証が可能であると判定し、ユーザ認証を代行するための、対応する送信データを前記Webサイト利用者認証用データ記憶部から取得し、前記Webサーバへ送信する代行認証用データ送信手段(217)と、を備える。ユーザ認証プロキシ装置における上記各手段は、ユーザ認証プロキシのデータ処理装置(コンピュータ)で実行されるプログラムにより、その処理・機能が実現され、該プログラムを記録した記録媒体(磁気ディスク、磁気テープ、光ディスク、もしくは半導体メモリ等)から該プログラムをデータ処理装置に読み出して実行することで、ユーザ認証プロキシ装置を実施することができる。

【0023】

【実施例】上記した本発明の実施の形態についてさらに詳細に説明すべく、本発明の実施例について図面を参照して以下に説明する。図1は、本発明の一実施例のシステム構成を示す図である。

【0024】図1を参照すると、本発明の一実施例は、有線あるいは無線によりインターネット3と相互に接続できる機能を有するパーソナルコンピュータ、携帯電話機、携帯情報端末、FAXなどのユーザ端末1と、インターネット3上でユーザ認証が必要なWebサイトを提供している情報処理装置であるWebサーバ4と、ユーザ端末1とインターネット3との接続を仲介する情報処理装置であるユーザ認証プロキシ2を含む。

【0025】図2は、本発明の一実施例におけるユーザ認証プロキシ2の構成の一例を示す図である。図2を参照すると、ユーザ認証プロキシ2は、プログラム制御により動作するデータ処理装置21と、情報を記憶する記憶装置22と、を含む。

【0026】記憶装置22は、プロキシ利用者認証用データ記憶部221と、Webサイト利用者認証用データ記憶部222と、を備えている。

【0027】プロキシ利用者認証用データ記憶部221には、ユーザ認証プロキシ2を利用する利用者が正当な利用者であることを確認するために必要な情報が記憶されている。

【0028】利用者は、Webサイトのユーザ認証を、ユーザ認証プロキシ2に代行させる前に、利用者自身が正当な利用者であることをユーザ認証プロキシ2に証明しなければならない。

【0029】Webサイト利用者認証用データ記憶部2

22には、利用者を一意に識別する識別子と、WebサイトのURLと、ユーザ認証用にユーザ端末1がWebサーバ4から受信したデータと、ユーザ認証用にユーザ端末1がWebサーバ4に送信したデータとの組が記憶されている。

【0030】データ処理装置21は、プロキシ利用者認証手段211と、URL保存手段212と、受信データ保存手段213と、送信データ保存手段214と、URL比較手段215と、受信データ比較手段216と、代行認証用データ送信手段217とを備えている。

【0031】プロキシ利用者認証手段211は、プロキシ利用者認証用データ記憶部221に保存されているデータを利用して、ユーザがユーザ認証プロキシ2の正当な利用者であるかどうかの認証を行う。

【0032】URL保存手段212は、ユーザがユーザ認証プロキシ2にユーザ認証を代行させるように指示したWebサイトのURLを、ユーザを一意に識別するための識別子と組にしてWebサイト利用者認証用データ記憶部222に保存する。

【0033】受信データ保存手段213は、ユーザ認証を行うためにユーザ端末1がWebサーバ4から受信したデータを、Webサイト利用者認証用データ記憶部222に保存する。

【0034】送信データ保存手段214は、ユーザ認証を行うためにユーザ端末1がWebサーバ4へ送信したデータを、Webサイト利用者認証用データ記憶部222に保存する。

【0035】URL比較手段215は、ユーザがユーザ端末1で指定したURLと、Webサイト利用者認証用データ記憶部222に保存されているURLとを比較し、ユーザ認証プロキシ2がユーザ認証を代行するURLであるかどうかを判断する。

【0036】受信データ比較手段216は、ユーザが指定したURLを使用して、その時点で実際にWebサーバ4に接続してWebサーバ4から受信したデータと、Webサイト利用者認証用データ記憶部222に保存されている受信データとを比較する。

【0037】代行認証用データ送信手段217は、ユーザ認証を代行するための送信データを、Webサイト利用者認証用データ記憶部222から取得し、Webサーバ4へ送信する。

【0038】本発明の一実施例におけるデータ処理装置21の上記各手段211～217は、データ処理装置21で実行されるプログラムによりその処理・機能が実現される。

【0039】次に図1乃至図8を参照して、本発明の一実施例の動作について詳細に説明する。

【0040】まず、ユーザがユーザ認証を代行させるためのデータをユーザ認証プロキシ2に保存する動作について、図3に示した流れ図を参照して、詳細に説明す

る。

【0041】ユーザは、ユーザ端末1を利用して、ユーザ認証代行に必要なデータの保存開始要求を、ユーザ認証プロキシ2に送信する(ステップA1)。

【0042】ユーザ認証プロキシ2のプロキシ利用者認証手段211は、ユーザがユーザ認証プロキシ2の正当なユーザであることを確認するために必要な認証用データを要求する(ステップA2)。

【0043】ユーザは、ユーザ端末1から、ユーザ認証プロキシ2の正当なユーザであることを示すデータを送信する(ステップA3)。

【0044】ユーザ認証プロキシ2のプロキシ利用者認証手段211は、ユーザ端末1から送信されたデータと、プロキシ利用者認証用データ記憶部221に保存されているデータとを比較して、当該ユーザが正当なユーザであるか否かを判定する(ステップA4)。

【0045】正当なユーザであると判定されなかった場合には、ユーザ認証プロキシ2は代行認証用データの保存開始要求を拒否する(ステップA5)。

【0046】一方、ステップA4において、正当なユーザであると判定された場合には、ユーザ認証プロキシ2は、代行認証用データの保存開始を許可する(ステップA6)。

【0047】図5は、プロキシ利用者認証用データ記憶部221に記憶されているデータの一例を示す図である。図5に示す例では、ユーザ認証プロキシ2のユーザを認証するデータとして、ユーザを一意に識別するためのユーザIDと、パスワードが用いられている。

【0048】ユーザがユーザIDとして、“00001”を指定し、パスワードとして、“pKi#1_”を指定した場合には、正当なユーザと認証され、それ以外のパスワードが指定された場合には、正当なユーザであるとは認証されない。

【0049】ユーザ認証プロキシ2の正当なユーザであると認証されたユーザは、ユーザ端末1から、Webサイトのユーザ認証用URL(uniform resource locator)を、ユーザ認証プロキシ2に送信する(ステップA7)。

【0050】ユーザ認証プロキシ2は、ユーザ端末1から送信されたURLを受け取り、URLをユーザを一意に識別するための識別子と組にして、一時記憶に記憶した上で、Webサーバ4に接続する(ステップA8)。

【0051】Webサーバ4は、ユーザ認証プロキシ2からURLを受信し、URLに対するデータを、ユーザ認証プロキシ2へ返信する(ステップA9)。

【0052】ユーザ認証プロキシ2は、Webサーバ4から受信したデータを、ユーザを一意に識別するための識別子およびURLと組にして一時記憶に記憶した上で、ユーザ端末1へデータを送信する(ステップA10)。

【0053】ユーザはユーザ端末1から、Webサイトのユーザ認証に必要なデータを、ユーザ認証プロキシ2へ送信する(ステップA11)。

【0054】ユーザ認証プロキシ2は、ユーザ端末1から送信されたWebサイトのユーザ認証用データを受け取り、これを、ユーザを一意に識別するための識別子およびURLと組にして一時記憶に記憶した上で、Webサーバ4へ送信する(ステップA12)。

【0055】Webサーバ4は、ユーザ認証プロキシ2から送信されたユーザ認証用データを検査し、Webサイトの正当なユーザであるか否かを判定する(ステップA13)。

【0056】Webサーバ4が、ユーザをWebサイトの正当なユーザではないと判定した場合には、ユーザ認証に失敗したことを、ユーザ認証プロキシ2を通して、ユーザ端末1に通知する(ステップA14)。

【0057】Webサーバ4が、ユーザをWebサイトの正当なユーザであると判定した場合には、ユーザ認証に成功したことを、ユーザ認証プロキシ2を通してユーザ端末1に通知する(ステップA15)。

【0058】Webサイトのユーザ認証に成功した場合、ユーザは、ユーザ端末1を利用して、代行認証用データの保存終了を、ユーザ認証プロキシ2へ送信する(ステップA16)。

【0059】ユーザ認証プロキシ2は、URL保存手段212、受信データ保存手段213、送信データ保存手段214を利用して、一時記憶に記憶されている、

- ・ユーザ識別子、
- ・URL、

- ・ユーザ端末1がWebサーバ4から受信したデータ、および、

- ・ユーザ端末1がWebサーバ4へ送信したデータを、Webサイト利用者認証用データ記憶部222へ保存する(ステップA17)。

【0060】図6は、Webサイト利用者認証用データ記憶部222に記憶されているデータの一例を示す図である。図6に示す例では、

- ・ユーザを一意に識別するためのユーザID、
- ・URL、

- ・Webサーバからの受信データ、および、
- ・Webサーバからの送信データ

の組が保存されている。

【0061】ユーザIDが“00001”のユーザに対しては、“http://www.nec.co.jp/customer.html”のURLに対する送受信データと、“http://www.shop1.co.jp/buyer.html”のURLに対する送受信データが保存されており、これら2つのURLで示されるWebサイトのユーザ認証をユーザ認証プロキシ2が代行できるように設定されている。

【0062】同様に、ユーザIDが“00002”のユ

ーザに対しては、"http://www.nec.co.jp/customer.html"のURLに対する送受信データと、"http://www.books.co.jp/buyer.html"のURLに対する送受信データが保存されており、これら2つのURLで示されるWebサイトのユーザ認証をユーザ認証プロキシ2が代行できるように設定されている。

【0063】図7は、図6における受信データ1および送信データ1の例を示す図である。Webサーバ4からの受信データ1として、HTML (HyperText Markup Language) のテキストが保存されている。このHTMLテキストにおいて、<FORM ACTION...>は、CGI (/cgi-bin) にデータを入力するためのタグであり、<table>タグにおいて、UserID欄、Password欄の表示と、入力(入力フォームは<input>で規定される)、及び、value="Submit"で規定されるSubmitボタンが表示され、Submitボタンの押下により、入力データがCGIに受け渡される。Webサーバ4へ送信する送信データ1としては、CGI (Common Gateway Interface) のPOSTメソッドで引き渡すテキスト(uid (ユーザ識別子) が00001でpwdがn#ilce_9) が保存されている。

【0064】図8は、図6における受信データ2および送信データ2の例を示す図である。図8に示す例では、Webサーバから受信したデータとして、XML (eXtensible Markup Language) のテキスト(<?xml:stylesheetで始まる行は、このXML文書を表示すべきXLT (eXtensible Stylesheet Language) スクリプトが"member.xml"であることを示す) が保存されており、Webサーバへ送信するデータとしても、XMLのテキストが保存されている。

【0065】次に、ユーザがユーザ認証プロキシ2を利用して、Webサイトのユーザ認証を代行させる動作を、図4の流れ図を参照して詳細に説明する。

【0066】ユーザは、ユーザ端末1から、ユーザ認証プロキシ2の使用を要求する(ステップB1)。

【0067】ユーザ認証プロキシ2において、プロキシ利用者認証手段211が、ユーザがユーザ認証プロキシ2の正当なユーザであることを確認するために必要な認証用データを要求する(ステップB2)。

【0068】ユーザは、ユーザ端末1から、ユーザ認証プロキシ2の正当なユーザであることを示すデータを送信する(ステップB3)。

【0069】ユーザ認証プロキシ2のプロキシ利用者認証手段211は、ユーザ端末1から受信したデータと、プロキシ利用者認証用データ記憶部221に保存されているデータとにより、ユーザが正当なユーザが否かを判定する(ステップB4)。

【0070】正当なユーザであると判定されなかった場合には、ユーザ認証プロキシ2はユーザの利用を拒否する(ステップB5)。

【0071】ステップB4において、正当なユーザであると判定された場合には、ユーザ認証プロキシ2はユーザの利用を許可する(ステップB6)。

【0072】図5は、プロキシ利用者認証用データ記憶部221に記憶されているデータの一例を示す図である。図5に示す例では、ユーザ認証プロキシ2のユーザを認証するデータとして、ユーザを一意に識別するためのユーザIDと、パスワードが用いられている。ユーザがユーザIDとして"00001"を指定し、パスワードとして"pKi#1_*)"を指定した場合には正当なユーザと認証され、それ以外のパスワードが指定された場合には正当なユーザであるとは認証されない。

【0073】ユーザ認証プロキシ2の正当なユーザであると認証されたユーザは、ユーザ端末1を利用してWebサイトのユーザ認証用URLをユーザ認証プロキシ2に送信する(ステップB7)。

【0074】ユーザ認証プロキシ2は、ユーザ端末1から受信したURLを、ユーザを一意に識別するための識別子と組にして一時記憶に記憶した上で、Webサーバ4に接続する(ステップB8)。

【0075】Webサーバ4は、ユーザ認証プロキシ2からURLを受信し、URLに対するデータをユーザ認証プロキシ2へ返信する(ステップB9)。

【0076】ユーザ認証プロキシ2は、Webサーバ4から受信したデータを、ユーザを一意に識別するための識別子およびURLと組にして一時記憶に記憶する(ステップB10)。

【0077】ユーザ認証プロキシ2は、URL比較手段215および受信データ比較手段216を利用して、一時記憶に記憶されているユーザ識別子、URL、およびWebサーバから受信した受信データの組が、Webサイト利用者認証用データ記憶部222に存在するか否かをチェックし、代行認証が可能か否かを判定する(ステップB11)。

【0078】一時記憶に記憶されているユーザ識別子、URL、およびWebサーバから受信した受信データの組が、Webサイト利用者認証用データ記憶部222に存在しない場合には、代行認証が不可能と判定し、Webサーバ4から受信したデータをそのままユーザ端末1へ返信する(ステップB12)。

【0079】一時記憶に記憶されているユーザ識別子、URL、およびWebサーバから受信した受信データの組が、Webサイト利用者認証用データ記憶部222に存在する場合には、代行認証が可能と判定し、代行認証用データ送信手段217を利用して、対応する送信データをWebサイト利用者認証用データ記憶部222から取得し、Webサーバ4へ送信する(ステップB1

3)。

【0080】図6および図7の例では、ユーザIDが“00001”のユーザが、“http://www.nec.co.jp/customer.html”のURLにアクセスした場合に、Webサーバが図7における受信データ1と同じテキストをユーザ認証プロキシ2に返却すると、ユーザ認証プロキシ2は、代行認証が可能と判定し、図7の送信データ1をWebサーバ4へ送信する。

【0081】図6および図8の例では、ユーザIDが“00001”のユーザが、“http://www.shop1.co.jp/buyer.html”のURLにアクセスした場合に、Webサーバが、図8における受信データ2と同じテキストをユーザ認証プロキシ2に返却すると、ユーザ認証プロキシ2は代行認証が可能と判定し、図8の送信データ2をWebサーバ4へ送信する。

【0082】

【発明の効果】以上説明したように本発明によれば下記記載の効果を奏する。

【0083】本発明の第1の効果は、ユーザ端末とWebサーバ間に、ユーザ認証を代行するプロキシを配置したことにより、ユーザ認証を必要とする任意のWebサイトに対して、シングルサインオン(singl e s i g n o n)によりユーザ認証を行うことができる、ということである。

【0084】前述したように、ユーザ認証を必要とするWebサイトは急速に増加しているが、ユーザを認証する方法は統一されていず、Webサイト毎に個別の方法を採用している場合が多いというのが現状であり、本発明によれば、このような個別のユーザ認証方法を採用しているWebサイトに対して、Webサイト提供者に何ら負担をかけることなく、シングルサインオンにより、ユーザ認証可能としており、本発明の有効性は顕著である。

【0085】また、本発明の第2の効果は、携帯電話や携帯情報端末をユーザ端末とするシステムにおいては、シングルサインオンによって必要なすべてのWebサイトにアクセス可能となり、ユーザ認証に必要な操作を大幅に削減し、ユーザの負担を軽減し、操作性、利便性を向上させる、ということである。

【0086】その理由は、本発明においては、ユーザ端

【図5】

ユーザID	パスワード
00001	pK#1_7
00002	sB-CK&1
...	...

末とWebサーバとの間にユーザ認証を行うプロキシを置き、ユーザ認証時にユーザ端末とWebサーバとの間で送受信されるデータを、そのままの形でプロキシに保存し、再利用しているためである。そして、Webサイトごとにユーザ認証の方法が異なる場合でも、実際にネットワークを流れるデータをそのままの形で保存しておくことで、ユーザ認証に再利用することができる、ためである。

【図面の簡単な説明】

【図1】本発明の一実施例の構成を示す図である。

【図2】本発明の一実施例におけるユーザ認証プロキシの構成を示す図である。

【図3】本発明の一実施例の動作を説明するための流れ図である。

【図4】本発明の一実施例の動作を説明するための流れ図である。

【図5】本発明の一実施例におけるプロキシ利用者認証用データ記憶部の内容の一例を示す図である。

【図6】本発明の一実施例におけるWebサイト利用者認証用データ記憶部の内容の一例を示す図である。

【図7】本発明の一実施例における受信データと送信データの一例を示す図である。

【図8】本発明の一実施例における受信データと送信データの一例を示す図である。

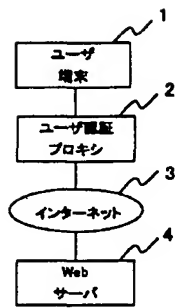
【符号の説明】

- 1 ユーザ端末
- 2 ユーザ認証プロキシ
- 3 インターネット
- 4 Webサーバ
- 21 データ処理装置
- 211 プロキシ利用者認証手段
- 212 URL保存手段
- 213 受信データ保存手段
- 214 送信データ保存手段
- 215 URL比較手段
- 216 受信データ比較手段
- 217 代行認証用データ送信手段
- 22 記憶装置
- 221 プロキシ利用者認証用データ記憶部
- 222 Webサイト利用者認証用データ記憶部

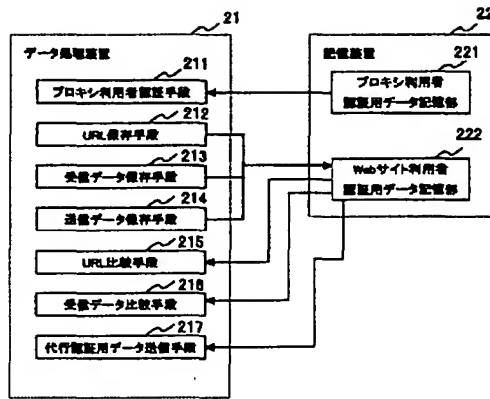
【図6】

ユーザID	URL	受信データ	送信データ
00001	http://www.nec.co.jp/customer.html	受信データ1	送信データ1
00001	http://www.shop1.co.jp/buyer.html	受信データ2	送信データ2
00002	http://www.nec.co.jp/customer.html	受信データ3	送信データ3
00002	http://www.shop1.co.jp/buyer.html	受信データ4	送信データ4
...

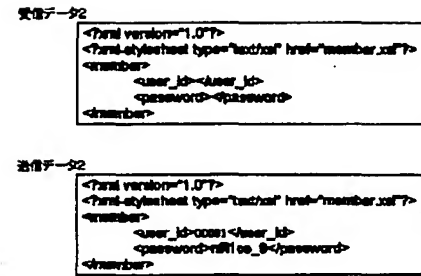
【図1】



【図2】



【図8】



【図7】

受信データ1

```

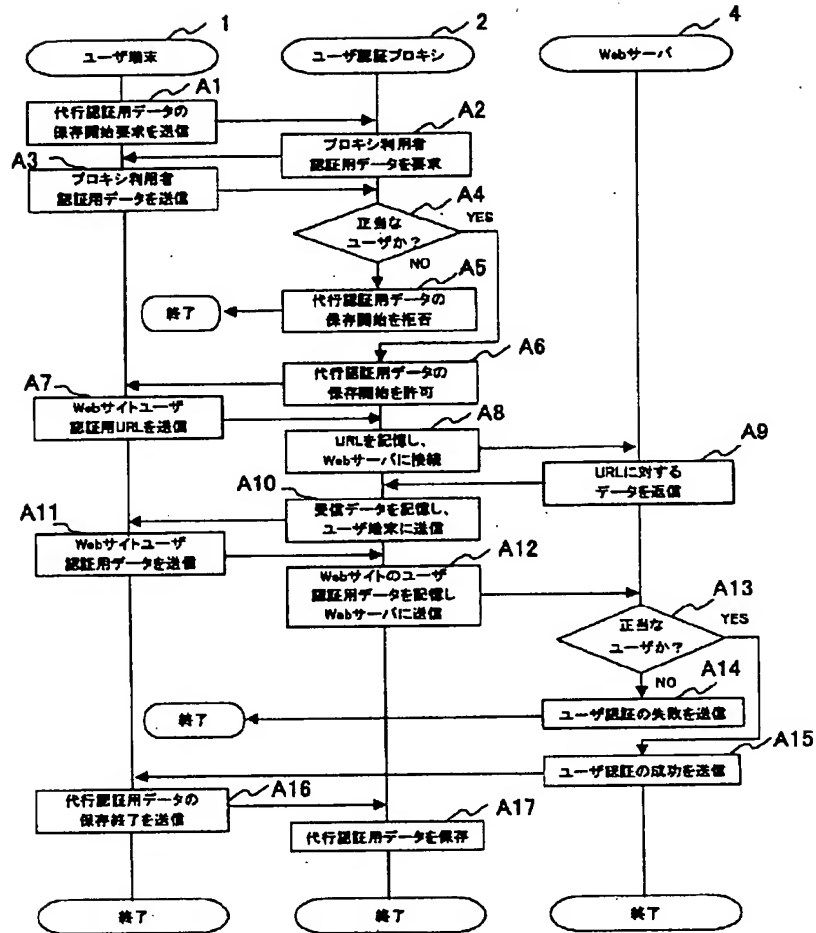
<HTML>
<BODY>
<FORM ACTION="/cgi-bin/member.cgi" METHOD="POST">
<table>
  <tr><td>User ID</td><td><input type="text" name="id"></td></tr>
  <tr><td>Password</td><td><input type="password" name="pwd"></td></tr>
  <tr><td><input type="submit" value="Submit"></td></tr>
</table>
</FORM>
</BODY>
</HTML>
  
```

送信データ1

```

id=00001&pwd=n81ee_0
  
```

【図3】



【図4】

